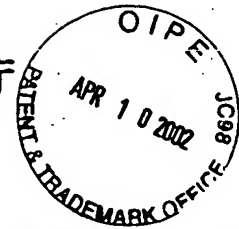


日本国特許庁  
JAPAN PATENT OFFICE



別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日

Date of Application:

2000年12月28日

出願番号

Application Number:

特願2000-402959

[ST.10/C]:

[JP2000-402959]

出願人

Applicant(s):

株式会社エヌ・ティ・ティ・ドコモ

RECEIVED

APR 12 2002

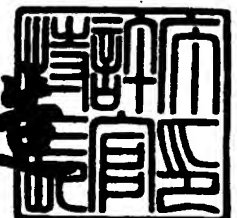
Technology Center 2100

CERTIFIED COPY OF  
PRIORITY DOCUMENT

2002年 2月15日

特許庁長官  
Commissioner,  
Japan Patent Office

及川耕造



出証番号 出証特2002-3007780

Docket No. 217759US2/sbj



#4

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

RE APPLICATION OF: Takashi SUZUKI, et al.

GAU: 2131

SERIAL NO: 10/026,640

EXAMINER:

FILED: December 27, 2001

FOR: CONTENT DISTRIBUTION SYSTEM, COPYRIGHT PROTECTION SYSTEM AND CONTENT RECEIVING TERMINAL

REQUEST FOR PRIORITY

ASSISTANT COMMISSIONER FOR PATENTS  
WASHINGTON, D.C. 20231

SIR:

- ☐ Full benefit of the filing date of U.S. Application Serial Number [US App No], filed [US App Dt], is claimed pursuant to the provisions of 35 U.S.C. §120.
- ☐ Full benefit of the filing date of U.S. Provisional Application Serial Number , filed , is claimed pursuant to the provisions of 35 U.S.C. §119(e).
- ☒ Applicants claim any right to priority from any earlier filed applications to which they may be entitled pursuant to the provisions of 35 U.S.C. §119, as noted below.

In the matter of the above-identified application for patent, notice is hereby given that the applicants claim as priority:

<u>COUNTRY</u>	<u>APPLICATION NUMBER</u>	<u>MONTH/DAY/YEAR</u>
JAPAN	2000-402959	December 28, 2000

Certified copies of the corresponding Convention Application(s)

- ☒ are submitted herewith
- ☐ will be submitted prior to payment of the Final Fee
- ☐ were filed in prior application Serial No. filed
- ☐ were submitted to the International Bureau in PCT Application Number .  
Receipt of the certified copies by the International Bureau in a timely manner under PCT Rule 17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.
- ☐ (A) Application Serial No.(s) were filed in prior application Serial No. filed ; and  
(B) Application Serial No.(s)
  - ☐ are submitted herewith
  - ☐ will be submitted prior to payment of the Final Fee

RECEIVED

APR 12 2002

Technology Center 2100



22850

Tel. (703) 413-3000  
Fax. (703) 413-2220  
(OSMMN 10/98)

Respectfully Submitted,

OBLON, SPIVAK, McCLELLAND,  
MAIER & NEUSTADT, P.C.

Marvin J. Spivak  
Registration No. 24,913

Joseph A. Scafetta, Jr.  
Registration No. 26,803

【書類名】 特許願

【整理番号】 ND12-0338

【提出日】 平成12年12月28日

【あて先】 特許庁長官 及川 耕造 殿

【国際特許分類】 H04L 12/00

【発明者】

【住所又は居所】 東京都千代田区永田町二丁目11番1号 株式会社エヌ・ティ・ティ・ドコモ内

【氏名】 鈴木 敬

【発明者】

【住所又は居所】 東京都千代田区永田町二丁目11番1号 株式会社エヌ・ティ・ティ・ドコモ内

【氏名】 河原 敏朗

【発明者】

【住所又は居所】 東京都千代田区永田町二丁目11番1号 株式会社エヌ・ティ・ティ・ドコモ内

【氏名】 栄藤 稔

【特許出願人】

【識別番号】 392026693

【氏名又は名称】 株式会社エヌ・ティ・ティ・ドコモ

【代理人】

【識別番号】 100070150

【弁理士】

【氏名又は名称】 伊東 忠彦

【手数料の表示】

【予納台帳番号】 002989

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】	図面	1
【物件名】	要約書	1
【プルーフの要否】	要	

【書類名】 明細書

【発明の名称】 コンテンツ配信システム、著作権保護システム及びコンテンツ受信端末

【特許請求の範囲】

【請求項 1】 コンテンツを保有し配信する 1 つ以上のコンテンツ配信サーバと、該コンテンツの著作権を保護する著作権保護システムと、該コンテンツ配信サーバからのコンテンツを受信するコンテンツ受信端末とを有するコンテンツ配信システムにおいて、

著作権保護システムは、

コンテンツの所在を示すコンテンツ所在情報を暗号化する暗号化手段と、

前記暗号化されたコンテンツ所在情報を含んだコンテンツ選択文書を生成するコンテンツ選択文書生成手段と、

前記生成したコンテンツ選択文書をコンテンツ受信端末へ送信するコンテンツ選択文書送信手段と、

を備え、

コンテンツ受信端末は、

著作権保護システムからのコンテンツ選択文書を受信するコンテンツ選択文書受信手段と、

前記受信したコンテンツ選択文書から暗号化されたコンテンツ所在情報を抽出するコンテンツ所在情報抽出手段と、

前記抽出した暗号化されたコンテンツ所在情報を復号する復号手段と、

前記復号したコンテンツ所在情報で指定されるコンテンツを保有するコンテンツ配信サーバに対して、コンテンツの配信要求を送出する配信要求送出手段と、

前記配信要求に応じてコンテンツ配信サーバから配信されるコンテンツを受信するコンテンツ受信手段と、

を備えるコンテンツ配信システム。

【請求項 2】 コンテンツを保有し配信する 1 つ以上のコンテンツ配信サーバと、該コンテンツの著作権を保護する著作権保護システムと、該コンテンツ配信サーバからのコンテンツを受信するコンテンツ受信端末とを有するコンテンツ

配信システムにおいて、

著作権保護システムは、

コンテンツの所在を示すコンテンツ所在情報と、コンテンツの所在の正当性を証明する所在認証情報とを含んだコンテンツ選択文書を生成するコンテンツ選択文書生成手段と、

前記生成したコンテンツ選択文書をコンテンツ受信端末へ送信するコンテンツ選択文書送信手段と、

を備え、

コンテンツ受信端末は、

著作権保護システムからのコンテンツ選択文書を受信するコンテンツ選択文書受信手段と、

前記受信したコンテンツ選択文書からコンテンツ選択文書と、所在認証情報とを抽出する情報抽出手段と、

前記抽出した所在認証情報に基づいて、コンテンツの所在の正当性を検証する正当性検証手段と、

前記検証によりコンテンツの所在の正当性が確認された場合に、前記抽出したコンテンツ所在情報で指定されるコンテンツを保有するコンテンツ配信サーバに対して、コンテンツの配信要求を送出する配信要求送出手段と、

前記配信要求に応じてコンテンツ配信サーバから配信されるコンテンツを受信するコンテンツ受信手段と、

を備えるコンテンツ配信システム。

【請求項 3】 コンテンツを保有し配信する 1 つ以上のコンテンツ配信サーバと、該コンテンツの著作権を保護する著作権保護システムと、該コンテンツ配信サーバからのコンテンツを受信するコンテンツ受信端末とを有するコンテンツ配信システムにおいて、

著作権保護システムは、

コンテンツの所在を示すコンテンツ所在情報を暗号化する暗号化手段と、

前記暗号化されたコンテンツ所在情報と、コンテンツの所在の正当性を証明する所在認証情報とを含んだコンテンツ選択文書を生成するコンテンツ選択文書生

成手段と、

前記生成したコンテンツ選択文書をコンテンツ受信端末へ送信するコンテンツ  
選択文書送信手段と、

を備え、

コンテンツ受信端末は、

著作権保護システムからのコンテンツ選択文書を受信するコンテンツ選択文書  
受信手段と、

前記受信したコンテンツ選択文書から暗号化されたコンテンツ所在情報と、所  
在認証情報とを抽出する情報抽出手段と、

前記抽出した暗号化されたコンテンツ所在情報を復号する復号手段と、

前記抽出した所在認証情報に基づいて、コンテンツの所在の正当性を検証する  
正当性検証手段と、

前記検証によりコンテンツの所在の正当性が確認された場合に、前記復号した  
コンテンツ所在情報で指定されるコンテンツを保有するコンテンツ配信サーバに  
対して、コンテンツの配信要求を送出する配信要求送出手段と、

前記配信要求に応じてコンテンツ配信サーバから配信されるコンテンツを受信  
するコンテンツ受信手段と、

を備えるコンテンツ配信システム。

【請求項 4】 請求項 3 に記載のコンテンツ配信システムにおいて、

前記暗号化手段は、前記コンテンツ所在情報と前記所在認証情報とをまとめて  
暗号化し、

前記コンテンツ選択文書生成手段は、前記暗号化データを含んだコンテンツ選  
択文書を生成し、

前記情報抽出手段は、前記受信したコンテンツ選択文書から暗号化データを抽  
出し、

前記復号手段は、前記抽出した暗号化データからコンテンツ所在情報と所在認  
証情報とを復号し、

前記正当性検証手段は、前記復号した所在認証情報に基づいて、コンテンツの  
所在の正当性を検証するようにしたコンテンツ配信システム。

【請求項 5】 コンテンツの著作権を保護する著作権保護システムにおいて

コンテンツの所在を示すコンテンツ所在情報を暗号化する暗号化手段と、  
前記暗号化されたコンテンツ所在情報を含んだコンテンツ選択文書を生成する  
コンテンツ選択文書生成手段と、  
前記生成したコンテンツ選択文書をコンテンツ受信端末へ送信するコンテンツ  
選択文書送信手段と、  
を備える著作権保護システム。

【請求項 6】 コンテンツの著作権を保護する著作権保護システムにおいて

コンテンツの所在を示すコンテンツ所在情報と、コンテンツの所在の正当性を  
証明する所在認証情報とを含んだコンテンツ選択文書を生成するコンテンツ選択  
文書生成手段と、  
前記生成したコンテンツ選択文書をコンテンツ受信端末へ送信するコンテンツ  
選択文書送信手段と、  
を備える著作権保護システム。

【請求項 7】 コンテンツの著作権を保護する著作権保護システムにおいて

コンテンツの所在を示す所在情報を暗号化する暗号化手段と、  
前記暗号化された所在情報と、コンテンツの所在の正当性を証明する所在認証  
情報とを含んだコンテンツ選択文書を生成するコンテンツ選択文書生成手段と、  
前記生成したコンテンツ選択文書をコンテンツ受信端末へ送信するコンテンツ  
選択文書送信手段と、  
を備える著作権保護システム。

【請求項 8】 請求項 7 に記載の著作権保護システムにおいて、

前記暗号化手段は、前記コンテンツ所在情報と前記所在認証情報とをまとめて  
暗号化し、

前記コンテンツ選択文書生成手段は、前記暗号化データを含んだコンテンツ選  
択文書を生成するようにした著作権保護システム。



【請求項 9】 請求項 5、7 又は 8 に記載の著作権保護システムにおいて、コンテンツ所在情報を含むコンテンツ情報、該コンテンツ情報に関連したアクセス情報及びコンテンツを利用するユーザ又はコンテンツ受信端末の正当性を証明するユーザ認証情報を取得する情報取得手段と、

前記取得したアクセス情報とユーザ認証情報に基づいてコンテンツ所在情報の暗号化方式を選択する暗号化方式選択手段と、  
を備え、

前記暗号化手段は、前記選択された暗号化方式を用いてコンテンツ所在情報を暗号化するようにした著作権保護システム。

【請求項 10】 請求項 6、7 又は 8 に記載の著作権保護システムにおいて

コンテンツ所在情報を含むコンテンツ情報、該コンテンツ情報に関連したアクセス情報及びコンテンツ所在情報で指定されるコンテンツの所在の正当性を証明する所在認証情報を取得する情報取得手段を備え、

コンテンツ選択文書生成手段は、前記取得された所在認証情報を含んだコンテンツ選択文書を生成するようにした著作権保護システム。

【請求項 11】 請求項 5、7 乃至 10 の何れかに記載の著作権保護システムにおいて、

前記暗号化されたコンテンツ所在情報を復号する鍵をコンテンツ受信端末と共有する鍵共有手段と、

前記鍵が共有された後にコンテンツ所在情報で指定されるコンテンツの利用料金を課金する課金手段と、  
を備える著作権保護システム。

【請求項 12】 暗号化されたコンテンツ所在情報を含んだコンテンツ選択文書を受信するコンテンツ選択文書受信手段と、

前記受信したコンテンツ選択文書からコンテンツ所在情報を抽出するコンテンツ所在情報抽出手段と、

前記抽出した暗号化されたコンテンツ所在情報を復号する復号手段と、

前記復号したコンテンツ所在情報で指定されるコンテンツを保有するコンテン

ッ配信サーバに対して、コンテンツの配信要求を送出する配信要求送出手段と、  
前記配信要求に応じてコンテンツ配信サーバから配信されるコンテンツを受信するコンテンツ受信手段と、  
を備えるコンテンツ受信端末。

【請求項 1 3】 コンテンツの所在を示すコンテンツ所在情報と、コンテンツの所在の正当性を証明する所在認証情報とを含んだコンテンツ選択文書を受信するコンテンツ選択文書受信手段と、

前記受信したコンテンツ選択文書からコンテンツ所在情報と、所在認証情報とを抽出する情報抽出手段と、

前記抽出した所在認証情報に基づいて、コンテンツの所在の正当性を検証する正当性検証手段と、

前記検証によりコンテンツの所在の正当性が確認された場合に、前記抽出したコンテンツ所在情報で指定されるコンテンツを保有するコンテンツ配信サーバに対して、コンテンツの配信要求を送出する配信要求送出手段と、

前記配信要求に応じてコンテンツ配信サーバから配信されるコンテンツを受信するコンテンツ受信手段と、  
を備えるコンテンツ受信端末。

【請求項 1 4】 暗号化されたコンテンツの所在を示すコンテンツ所在情報と、コンテンツの所在の正当性を証明する所在認証情報とを含んだコンテンツ選択文書を受信するコンテンツ選択文書受信手段と、

前記受信したコンテンツ選択文書から暗号化されたコンテンツ所在情報と、所在認証情報とを抽出する情報抽出手段と、

前記抽出した暗号化されたコンテンツ所在情報を復号する復号手段と、

前記抽出した所在認証情報に基づいて、コンテンツの所在の正当性を検証する正当性検証手段と、

前記検証によりコンテンツの所在の正当性が確認された場合に、前記復号したコンテンツ所在情報で指定されるコンテンツを保有するコンテンツ配信サーバに対して、コンテンツの配信要求を送出する配信要求送出手段と、

前記配信要求に応じてコンテンツ配信サーバから配信されるコンテンツを受信

するコンテンツ受信手段と、  
を備えるコンテンツ受信端末。

【請求項 1 5】 請求項 1 4 に記載のコンテンツ受信端末において、  
前記情報抽出手段は、前記受信したコンテンツ選択文書から暗号化データを抽出し、

前記復号手段は、前記抽出した暗号化データからコンテンツ所在情報と所在認証情報とを復号し、

前記正当性検証手段は、前記復号した所在認証情報に基づいて、コンテンツの所在の正当性を検証するようにしたコンテンツ受信端末。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は、著作物であるコンテンツの著作権を保護するためのシステムに関し、特に、著作物であるコンテンツを配信するコンテンツ配信システムにおける著作物保護技術に関する。

【0 0 0 2】

【従来技術】

近年、高速なアクセス回線の普及やインターネット技術の発展に伴い、映像や音楽等のコンテンツをインターネット経由で配信するコンテンツ配信サービスが実現されている。このようなコンテンツ配信サービスを普及させるためには、著作物であるコンテンツの所有者に対して適正な対価が支払われることが不可欠である。このため、コンテンツの利用者に対し課金を行うシステムが必要となる。

【0 0 0 3】

コンテンツの利用量に応じて利用者に対し課金するコンテンツ配信システムには、例えば公開特許公報「特開 2 0 0 0 ー 1 0 1 5 7 3」に開示されたシステムがある。この「特開 2 0 0 0 ー 1 0 1 5 7 3」に開示されたコンテンツ配信システムでは、サーバがコンテンツ受信端末の要求に応じてコンテンツの配信処理を行うとともに、サーバにおいてコンテンツ利用に対する課金処理を行っている。

【0 0 0 4】

## 【発明が解決しようとする課題】

ところで、サービス利用者が多い大規模なコンテンツ配信システムでは、ユーザ認証及び課金処理とコンテンツの配信処理とを同一のサーバで行うと、ユーザ認証及び課金処理の負担が大きいと、同時に配信可能なユーザ数が減少する等の問題が生じる。従って、サーバの負荷分散のため、ユーザ認証及び課金処理とコンテンツの配信処理とを異なるサーバで分散する必要が生じる。また、このような負荷分散を図ることで、コンテンツ保有者とコンテンツ利用に対する課金業者とを別々にすることができ、より多様なコンテンツ配信サービスが可能になるという効果もある。

## 【0005】

このように負荷分散を図ったコンテンツ配信システムとしては、例えば図8に示すような構成が考えられる。図8において、認証・課金サーバ200は、コンテンツへのリンク情報が含まれるコンテンツ選択文書201を蓄積している。コンテンツ選択文書201は、例えばHTML形式の文書であり、リンク情報で示されるコンテンツが有料の場合には文書全体が暗号化され、無料の場合には暗号化されずに、コンテンツ受信端末100へ送信される。

## 【0006】

このため、上述の「特開2000-101573」に開示されたコンテンツ配信システムにおいて、認証・課金サーバとコンテンツ配信サーバとを分離した場合、個々のコンテンツに対し課金を行うためには、コンテンツの課金種別毎にコンテンツ選択文書を用意する必要がある。即ち、無料コンテンツを希望するユーザには、暗号化されていない無料コンテンツの選択文書を配布し、有料コンテンツについても希望するユーザには、暗号化されていない無料コンテンツの選択文書と暗号化された有料コンテンツの選択文書の双方を配布する必要があり、効率的ではなかった。

## 【0007】

また、「特開2000-101573」に開示されたコンテンツ配信システムでは、認証・課金サーバとコンテンツ配信サーバとを分離した場合、コンテンツ配信サーバに対する認証機構を備えていないことが問題となり得る。例えば、不

正なコンテンツサーバを示すリンク情報がコンテンツ選択文書に埋め込まれた場合、コンテンツ受信端末は、その不正なサーバへコンテンツ配信を要求することになり、違法コピーされたコンテンツが配信され、適切な課金が困難になる等の問題が生じ得る。

#### 【0008】

本発明は、上記問題点を解決するものであり、その目的は、大規模なシステムを構築可能であるとともに、コンテンツ課金を適正に行うことができるコンテンツ配信システム、著作権保護システム及びコンテンツ受信端末を提供することにある。

#### 【0009】

##### 【課題を解決するための手段】

上記の目的を達成するため、本発明は請求項1に記載されるように、コンテンツを保有し配信する1つ以上のコンテンツ配信サーバと、該コンテンツの著作権を保護する著作権保護システムと、該コンテンツ配信サーバからのコンテンツを受信するコンテンツ受信端末とを有するコンテンツ配信システムにおいて、著作権保護システムは、コンテンツの所在を示すコンテンツ所在情報を暗号化する暗号化手段と、前記暗号化されたコンテンツ所在情報を含んだコンテンツ選択文書を生成するコンテンツ選択文書生成手段と、前記生成したコンテンツ選択文書をコンテンツ受信端末へ送信するコンテンツ選択文書送信手段とを備え、コンテンツ受信端末は、著作権保護システムからのコンテンツ選択文書を受信するコンテンツ選択文書受信手段と、前記受信したコンテンツ選択文書から暗号化されたコンテンツ所在情報を抽出するコンテンツ所在情報抽出手段と、前記抽出した暗号化されたコンテンツ所在情報を復号する復号手段と、前記復号したコンテンツ所在情報で指定されるコンテンツを保有するコンテンツ配信サーバに対して、コンテンツの配信要求を送出する配信要求送出手段と、前記配信要求に応じてコンテンツ配信サーバから配信されるコンテンツを受信するコンテンツ受信手段とを備える。

#### 【0010】

このように、コンテンツ配信サーバと著作権保護システムが分離され、且つ、

コンテンツの配信に際してコンテンツ配信サーバと著作権保護システムとの間で情報のやり取りが行われることがないため、コンテンツ配信サーバの負荷を軽減させて、大規模なコンテンツ配信システムを構築することができる。

## 【 0 0 1 1 】

また、従来のようにコンテンツ選択文書全体が暗号化されるのではなく、コンテンツ所在情報だけを選択的に暗号化することが可能であるため、例えば課金種別に応じて暗号化された複数のコンテンツ所在情報をコンテンツ選択文書に含ませておくことで、効率的なコンテンツ課金を行うことができる。

## 【 0 0 1 2 】

また、本発明は請求項 2 に記載されるように、コンテンツを保有し配信する 1 つ以上のコンテンツ配信サーバと、該コンテンツの著作権を保護する著作権保護システムと、該コンテンツ配信サーバからのコンテンツを受信するコンテンツ受信端末とを有するコンテンツ配信システムにおいて、著作権保護システムは、コンテンツの所在を示すコンテンツ所在情報と、コンテンツの所在の正当性を証明する所在認証情報とを含んだコンテンツ選択文書を生成するコンテンツ選択文書生成手段と、前記生成したコンテンツ選択文書をコンテンツ受信端末へ送信するコンテンツ選択文書送信手段とを備え、コンテンツ受信端末は、著作権保護システムからのコンテンツ選択文書を受信するコンテンツ選択文書受信手段と、前記受信したコンテンツ選択文書からコンテンツ選択文書と、所在認証情報とを抽出する情報抽出手段と、前記抽出した所在認証情報に基づいて、コンテンツの所在の正当性を検証する正当性検証手段と、前記検証によりコンテンツの所在の正当性が確認された場合に、前記抽出したコンテンツ所在情報で指定されるコンテンツを保有するコンテンツ配信サーバに対して、コンテンツの配信要求を送出する配信要求送出手段と、前記配信要求に応じてコンテンツ配信サーバから配信されるコンテンツを受信するコンテンツ受信手段とを備える。

## 【 0 0 1 3 】

このように、コンテンツ配信サーバと著作権保護システムが分離され、且つ、コンテンツの配信に際してコンテンツ配信サーバと著作権保護システムとの間で情報のやり取りが行われることがないため、コンテンツ配信サーバの負荷を軽減

させて、大規模なコンテンツ配信システムを構築することができる。また、著作権保護システムからコンテンツ受信端末へコンテンツ所在情報とコンテンツの所在の正当性を証明する所在認証情報とが送信されるため、コンテンツ受信端末は、コンテンツ所在情報で示されるコンテンツの所在の正当性を検証することができる、不正なサーバへアクセスして配信を受けることが防止され適切な課金処理を行うことができる。

## 【 0 0 1 4 】

また、本発明は請求項 3 に記載されるように、コンテンツを保有し配信する 1 つ以上のコンテンツ配信サーバと、該コンテンツの著作権を保護する著作権保護システムと、該コンテンツ配信サーバからのコンテンツを受信するコンテンツ受信端末とを有するコンテンツ配信システムにおいて、著作権保護システムは、コンテンツの所在を示すコンテンツ所在情報を暗号化する暗号化手段と、前記暗号化されたコンテンツ所在情報と、コンテンツの所在の正当性を証明する所在認証情報とを含んだコンテンツ選択文書を生成するコンテンツ選択文書生成手段と、前記生成したコンテンツ選択文書をコンテンツ受信端末へ送信するコンテンツ選択文書送信手段とを備え、コンテンツ受信端末は、著作権保護システムからのコンテンツ選択文書を受信するコンテンツ選択文書受信手段と、前記受信したコンテンツ選択文書から暗号化されたコンテンツ所在情報と、所在認証情報とを抽出する情報抽出手段と、前記抽出した暗号化されたコンテンツ所在情報を復号する復号手段と、前記抽出した所在認証情報に基づいて、コンテンツの所在の正当性を検証する正当性検証手段と、前記検証によりコンテンツの所在の正当性が確認された場合に、前記復号したコンテンツ所在情報で指定されるコンテンツを保有するコンテンツ配信サーバに対して、コンテンツの配信要求を送出する配信要求送出手段と、前記配信要求に応じてコンテンツ配信サーバから配信されるコンテンツを受信するコンテンツ受信手段とを備える。

## 【 0 0 1 5 】

この場合には、請求項 1 及び 2 に記載された発明と同様、コンテンツ配信サーバと著作権保護システムが分離され、且つ、コンテンツの配信に際してコンテンツ配信サーバと著作権保護システムとの間で情報のやり取りが行われることがな

いため、コンテンツ配信サーバの負荷を軽減させて、大規模なコンテンツ配信システムを構築することができる。

【0016】

また、請求項1に記載された発明と同様、コンテンツ選択文書全体が暗号化されるのではなく、コンテンツ所在情報だけを選択的に暗号化することが可能であるため、例えば課金種別に応じて暗号化された複数のコンテンツ所在情報をコンテンツ選択文書に含ませておくことで、効率的なコンテンツ課金を行うことができる。

【0017】

また、請求項2に記載された発明と同様、著作権保護システムからコンテンツ受信端末へコンテンツの所在の正当性を証明する所在認証情報が送信されるため、コンテンツ受信端末は、コンテンツ所在情報で示されるコンテンツの所在の正当性を検証することができ、不正なサーバへアクセスして配信を受けることが防止され適切な課金処理を行うことができる。

【0018】

この場合、請求項4に記載されるように、前記コンテンツ配信システムにおいて、前記暗号化手段は、前記コンテンツ所在情報と前記所在認証情報とをまとめて暗号化し、前記コンテンツ選択文書生成手段は、前記暗号化データを含んだコンテンツ選択文書を生成し、前記情報抽出手段は、前記受信したコンテンツ選択文書から暗号化データを抽出し、前記復号手段は、前記抽出した暗号化データからコンテンツ所在情報と所在認証情報とを復号し、前記正当性検証手段は、前記復号した所在認証情報に基づいて、コンテンツの所在の正当性を検証することができる。

【0019】

また、請求項5乃至11に記載された著作権保護システムは、上述した請求項1乃至4に記載されたコンテンツ配信システムに適した著作権保護システムである。具体的には、本発明は請求項5に記載されるように、コンテンツの著作権を保護する著作権保護システムにおいて、コンテンツの所在を示すコンテンツ所在情報を暗号化する暗号化手段と、前記暗号化されたコンテンツ所在情報を含ん



だコンテンツ選択文書を生成するコンテンツ選択文書生成手段と、前記生成したコンテンツ選択文書をコンテンツ受信端末へ送信するコンテンツ選択文書送信手段とを備える。

【0020】

また、本発明は請求項6に記載されるように、コンテンツの著作権を保護する著作権保護システムにおいて、コンテンツの著作権を保護する著作権保護システムにおいて、コンテンツの所在を示すコンテンツ所在情報と、コンテンツの所在の正当性を証明する所在認証情報とを含んだコンテンツ選択文書を生成するコンテンツ選択文書生成手段と、前記生成したコンテンツ選択文書をコンテンツ受信端末へ送信するコンテンツ選択文書送信手段とを備える。

【0021】

また、本発明は請求項7に記載されるように、コンテンツの著作権を保護する著作権保護システムにおいて、コンテンツの所在を示す所在情報を暗号化する暗号化手段と、前記暗号化された所在情報と、コンテンツの所在の正当性を証明する所在認証情報とを含んだコンテンツ選択文書を生成するコンテンツ選択文書生成手段と、前記生成したコンテンツ選択文書をコンテンツ受信端末へ送信するコンテンツ選択文書送信手段とを備える。

【0022】

この場合、請求項8に記載されるように、前記著作権保護システムにおいて、前記暗号化手段は、前記暗号化手段は、前記コンテンツ所在情報と前記所在認証情報とをまとめて暗号化し、前記コンテンツ選択文書生成手段は、前記暗号化データを含んだコンテンツ選択文書を生成することができる。

【0023】

また、本発明は請求項9に記載されるように、請求項5、7又は8に記載の著作権保護システムにおいて、コンテンツ所在情報を含むコンテンツ情報、該コンテンツ情報に関連したアクセス情報及びコンテンツを利用するユーザ又はコンテンツ受信端末の正当性を証明するユーザ認証情報を取得する情報取得手段と、前記取得したアクセス情報とユーザ認証情報に基づいてコンテンツ所在情報の暗号化方式を選択する暗号化方式選択手段とを備え、前記暗号化手段は、前記選択さ

れた暗号化方式を用いてコンテンツ所在情報を暗号化する。

【0024】

また、本発明は請求項10に記載されるように、請求項6、7又は8に記載の著作権保護システムにおいて、コンテンツ所在情報を含むコンテンツ情報、該コンテンツ情報に関連したアクセス情報及びコンテンツ所在情報で指定されるコンテンツの所在の正当性を証明する所在認証情報を取得する情報取得手段を備え、コンテンツ選択文書生成手段は、前記取得された所在認証情報を含んだコンテンツ選択文書を生成する。

【0025】

また、本発明は請求項11に記載されるように、請求項5、7乃至10の何れかに記載の著作権保護システムにおいて、前記暗号化されたコンテンツ所在情報を復号する鍵をコンテンツ受信端末と共有する鍵共有手段と、前記鍵が共有された後にコンテンツ所在情報で指定されるコンテンツの利用料金を課金する課金手段とを備える。

【0026】

また、請求項12乃至15に記載されたコンテンツ受信端末は、上述した請求項1乃至4に記載されたコンテンツ配信システムに適したコンテンツ受信端末である。具体的には、本発明のコンテンツ受信端末は請求項12に記載されるように、暗号化されたコンテンツ所在情報を含んだコンテンツ選択文書を受信するコンテンツ選択文書受信手段と、前記受信したコンテンツ選択文書からコンテンツ所在情報を抽出するコンテンツ所在情報抽出手段と、前記抽出した暗号化されたコンテンツ所在情報を復号する復号手段と、前記復号したコンテンツ所在情報で指定されるコンテンツを保有するコンテンツ配信サーバに対して、コンテンツの配信要求を送出する配信要求送出手段と、前記配信要求に応じてコンテンツ配信サーバから配信されるコンテンツを受信するコンテンツ受信手段とを備える。

【0027】

また、本発明のコンテンツ受信端末は請求項13に記載されるように、コンテンツの所在を示すコンテンツ所在情報と、コンテンツの所在の正当性を証明する所在認証情報とを含んだコンテンツ選択文書を受信するコンテンツ選択文書受信

手段と、前記受信したコンテンツ選択文書からコンテンツ所在情報と、所在認証情報とを抽出する情報抽出手段と、前記抽出した所在認証情報に基づいて、コンテンツの所在の正当性を検証する正当性検証手段と、前記検証によりコンテンツの所在の正当性が確認された場合に、前記抽出したコンテンツ所在情報で指定されるコンテンツを保有するコンテンツ配信サーバに対して、コンテンツの配信要求を送出する配信要求送出手段と、前記配信要求に応じてコンテンツ配信サーバから配信されるコンテンツを受信するコンテンツ受信手段とを備える。

#### 【0028】

また、本発明のコンテンツ受信端末は請求項14に記載されるように、暗号化されたコンテンツの所在を示すコンテンツ所在情報と、コンテンツの所在の正当性を証明する所在認証情報とを含んだコンテンツ選択文書を受信するコンテンツ選択文書受信手段と、前記受信したコンテンツ選択文書から暗号化されたコンテンツ所在情報と、所在認証情報とを抽出する情報抽出手段と、前記抽出した暗号化されたコンテンツ所在情報を復号する復号手段と、前記抽出した所在認証情報に基づいて、コンテンツの所在の正当性を検証する正当性検証手段と、前記検証によりコンテンツの所在の正当性が確認された場合に、前記復号したコンテンツ所在情報で指定されるコンテンツを保有するコンテンツ配信サーバに対して、コンテンツの配信要求を送出する配信要求送出手段と、前記配信要求に応じてコンテンツ配信サーバから配信されるコンテンツを受信するコンテンツ受信手段とを備える。

#### 【0029】

この場合、請求項15に記載されるように前記コンテンツ受信端末において、前記情報抽出手段は、前記受信したコンテンツ選択文書から暗号化データを抽出し、前記復号手段は、前記抽出した暗号化データからコンテンツ所在情報と所在認証情報とを復号し、前記正当性検証手段は、前記復号した所在認証情報に基づいて、コンテンツの所在の正当性を検証することができる。

#### 【0030】

##### 【発明の実施の形態】

以下、本発明の実施の形態を図面に基づいて説明する。図1は、本発明の第1

実施例に係るコンテンツ配信システムの構成例を示す図である。同図に示すコンテンツ配信システム 1 0 0 0 は、コンテンツ受信端末 1 1 0 0、コンテンツサーバ群 1 2 0 0、著作権保護システム 1 3 0 0 を備えて構成される。コンテンツ受信端末 1 1 0 0 と、コンテンツサーバ群 1 2 0 0 及び著作権保護システム 1 3 0 0 とは、ネットワーク 1 5 0 0 を介して接続される。

#### 【 0 0 3 1 】

コンテンツ配信システム 1 0 0 0 では、著作権保護システム 1 3 0 0 がオーディオビジュアルデータであるコンテンツの所在を示すコンテンツ所在情報を暗号化して送信しており、この暗号化されたコンテンツ所在情報を受信したコンテンツ受信端末 1 1 0 0 が、復号鍵を保有する場合にのみ、暗号化されたコンテンツ所在情報を復号し、コンテンツサーバ群 1 2 0 0 にアクセスすることでコンテンツの配信を受けることができるようになっている。また、コンテンツ配信システム 1 0 0 0 では、著作権保護システム 1 3 0 0 がコンテンツの所在の正当性を証明する所在認証情報を保有し、これを送信しており、この所在認証情報を取得したコンテンツ受信端末 1 1 0 0 が、コンテンツの所在の正当性を検証することができるようになっている。

#### 【 0 0 3 2 】

著作権保護システム 1 3 0 0 は、コンテンツ選択文書 1 4 0 0 を生成し、コンテンツ受信端末 1 1 0 0 へ送信する機能を有する。図 2 は、第 1 実施例に係る著作権保護システム 1 3 0 0 の構成例を示す図である。

#### 【 0 0 3 3 】

コンテンツ受信端末 1 1 0 0 は、コンテンツの配信を受ける際、ユーザの操作により著作権保護システム 1 3 0 0 にアクセスする。このとき端末認証部 1 3 0 2 は、著作権保護システム 1 3 0 0 にアクセスするコンテンツ受信端末 1 1 0 0 又は該コンテンツ受信端末 1 1 0 0 のユーザの認証を行う。認証にはコンテンツ受信端末 1 1 0 0 又は該コンテンツ受信端末 1 1 0 0 のユーザに付与された ID とパスワードを用いた方法等を利用することができる。

#### 【 0 0 3 4 】

著作権保護システム 1 3 0 0 の内部で生成若しくは外部から入力されたコンテ

ンツ所在情報 1 3 0 8 には、コンテンツ配信サーバの正当性を証明する所在認証情報 1 3 1 1 が付与される。この際、所在認証情報であることを示すタグが所在認証情報タグ付加部 1 3 1 2 により付加される。所在認証情報の発行元には、著作権保護システム 1 3 0 0、コンテンツ配信サーバ運用者、コンテンツホルダとかが考えられるが、本実施例では著作権保護システム 1 3 0 0 を発行元とする。

#### 【 0 0 3 5 】

また、所在認証情報 1 3 1 1 の生成や検証には、公開鍵暗号系を適用したデジタル署名等を利用することができる。この場合、コンテンツ所在情報 1 3 0 8 に一方向性関数を施し、その演算結果を公開鍵暗号方式の秘密鍵を用いて暗号化したものを所在認証情報 1 3 1 1 とする。コンテンツ所在情報 1 3 0 8 を検証する場合には、受け取ったコンテンツ所在情報に一方向性関数を施した結果と、受け取った所在認証情報 1 3 1 1 を秘密鍵に対応する公開鍵で復号した結果とを比較する。そして、これらが一致すれば合格、一致しなければ不合格と判定する。デジタル署名については、辻井、笠原著「暗号と情報セキュリティ」P 1 3 0 ~ 1 4 7 に詳しい。

#### 【 0 0 3 6 】

所在認証情報タグ付加部 1 3 1 2 は、所在認証情報 1 3 1 1 に、所在認証情報であることを示すタグ（以下「所在認証情報タグ」と称する）を付加する。情報付加部 1 3 1 4 は、コンテンツ所在情報 1 3 0 8 に、所在認証情報タグ付加部 1 3 1 2 から出力される、所在認証情報 1 3 1 1 と所在認証情報タグとを付加する。

#### 【 0 0 3 7 】

暗号化部 1 3 0 9 は、情報付加部 1 3 1 4 から出力される、所在認証情報 1 3 1 1 が付加されたコンテンツ所在情報 1 3 0 8 を、コンテンツの課金種別に対応する暗号化鍵 1 3 0 7 により暗号化し、この暗号化したコンテンツ所在情報に、コンテンツ所在情報が暗号化されていることを示すタグ（以下「暗号化情報タグ」と称する）を付加する。

#### 【 0 0 3 8 】

コンテンツ所在情報の暗号化には、DES や TDES などを適用することがで

きる。また暗号化に用いられる暗号化鍵 1 3 0 7 は、所在情報暗号化鍵共有部 1 3 0 3 において、コンテンツ受信端末 1 1 0 0 と共有される。暗号化鍵 1 3 0 7 の共有には、D e f f i e - H e l l m a n (今井秀樹他著「情報セキュリティ理論」P 1 3 2 ~ 1 3 5 参照) の鍵配送アルゴリズム等を利用することができる。また、所在情報暗号化鍵共有部 1 3 0 3 は、コンテンツ受信端末 1 1 0 0 との間で共有される暗号化鍵 1 3 0 7 の共有履歴を記録しており、この共有履歴を課金部 1 3 0 6 に提供する。

#### 【0 0 3 9】

コンテンツ選択文書生成部 1 3 1 0 は、暗号化されたコンテンツ所在情報 1 3 0 8 を複数組み合わせるコンテンツ選択文書を生成する。署名部 1 3 1 3 は、コンテンツ選択文書の送信元となる著作権保護システム 1 3 0 0 の正当性を証明するために、生成されたコンテンツ選択文書に対し著作権保護システム 1 3 0 0 に対応する署名を付加する。コンテンツ選択文書配信部 1 3 0 4 は、この署名が付加されたコンテンツ選択文書を、上述した端末認証部 1 3 0 2 によって認証されたコンテンツ受信端末 1 1 0 0 へ配信する。

#### 【0 0 4 0】

再び図 1 に戻って説明する。コンテンツ受信端末 1 1 0 0 へ配信されるコンテンツ選択文書は、例えば同図に示すコンテンツ選択文書 1 4 0 0 の構成を有している。コンテンツ選択文書 1 4 0 0 は、無料コンテンツである音楽データ及びビデオデータに対応するコンテンツ所在情報及び所在認証情報を含んだ情報群 1 4 0 1 と、有料コンテンツである音楽データ及びビデオデータに対応するコンテンツ所在情報及び所在認証情報を含んだ情報群 1 4 0 2 と、コンテンツ選択文書 1 4 0 0 の送信元を証明する署名(コンテンツ選択文書署名) 1 4 0 4 を含んでいる。このコンテンツ選択文書 1 4 0 0 において、無料コンテンツである音楽データ及びビデオデータに対応するコンテンツ所在情報は、不特定多数のコンテンツ受信端末が配信を受けることができるように暗号化されておらず、有料コンテンツである音楽データ及びビデオデータに対応するコンテンツ所在情報のみが暗号化されている。なお、コンテンツ選択文書 1 4 0 0 には、コンテンツ所在情報及び所在認証情報とともに暗号化情報タグ及び所在認証情報タグが含まれるが、図

1ではこれらを省略している。

【0041】

課金部1306は、所在情報暗号化鍵共有部1303から提供される鍵共有履歴に基づいて、コンテンツ受信端末1100へ配信したコンテンツ選択文書内のコンテンツ所在情報を暗号化するために用いた暗号化鍵1307を認識し、この鍵1307に対応する課金種別に応じて、コンテンツ受信端末1100のユーザ、即ちコンテンツ利用者に対して課金を行う。コンテンツ利用者の特定に際して課金部1306は、端末認証部1302から提供されるコンテンツ受信端末1100又はユーザの識別情報を利用する。識別情報としては端末認証部1302による認証の際に用いられるコンテンツ受信端末1100又は該コンテンツ受信端末1100のユーザに付与されたIDが利用される。

【0042】

なお、課金部1306は、課金に際して、鍵共有履歴を用いる他に、コンテンツサーバ群1200の各コンテンツ配信サーバがコンテンツ受信端末1100に対し、コンテンツを配信した履歴を用いることもできる。この場合、アクセス情報受信部1301は、コンテンツサーバ群1200内のコンテンツ配信サーバからの配信履歴を受信する。課金部1306は、この受信された配信履歴に基づいてコンテンツ受信端末1100のユーザに対して課金を行う。

【0043】

課金部1306による課金処理の結果は、課金情報として課金情報蓄積サーバ1305に蓄積される。

【0044】

このように、課金に際して暗号化鍵1307の共有履歴とコンテンツの配信履歴とを使い分けることにより、様々な課金形態を実現することができる。例えば、暗号化鍵1307の共有履歴を用いた場合には、一度課金された後は何度もコンテンツの配信を可能とする定額サービスを実現することができる。また、シンボリックリンク等を用いてコンテンツ所在情報に一定の有効期間をもたせることで、その有効期間内であれば何度もコンテンツの配信を可能とする期間限定の定額サービスを実現することもできる。一方、コンテンツの配信履歴を用いた場合

には、配信する毎に課金する所謂ペイパービュー (Pay per View) のサービスを実現することができる。

#### 【0045】

図3は、第1実施例に係るコンテンツ受信端末1100の構成例を示す図である。端末認証部1101は、コンテンツの配信を受ける際、ユーザの操作に応じて著作権保護システム1300内の端末認証部1302に対し、認証に必要な情報（例えばコンテンツ受信端末1100又は該コンテンツ受信端末1100のユーザに付与されたIDとパスワード等）を送信することにより、該端末認証1302とともに認証処理を行う。

#### 【0046】

このような認証の後、著作権保護システム1300内のコンテンツ選択文書配信部1304からコンテンツ選択文書1400が送信される。コンテンツ選択文書受信部1102は、このコンテンツ選択文書1400を受信する。コンテンツ選択文書検証部1108は、コンテンツ選択文書1400に含まれている署名を検証することにより、該コンテンツ選択文書1400の正当性を検証する。正当性が検証できた場合には、コンテンツ選択文書検証部1108は、このコンテンツ選択文書1400をコンテンツ選択メニュー表示部1110へ出力する。コンテンツ選択メニュー表示部1110は、入力されたコンテンツ選択文書1400に基づいて、コンテンツ受信端末1100のユーザがコンテンツを選択するための画面（コンテンツ選択画面）を表示する。

#### 【0047】

コンテンツ受信端末1100のユーザは、コンテンツ選択画面で配信を受けたいコンテンツを選択する。選択結果は、ユーザ選択受信部1111で受信される。所在情報暗号化復号部1112は、ユーザによって選択されたコンテンツに対応するコンテンツ所在情報及び所在認証情報を、受信したコンテンツ選択文書1400から抽出する。所在情報暗号化復号部1112は、コンテンツ選択文書1400に含まれる暗号化情報タグにより抽出したコンテンツ所在情報及び所在認証情報が暗号化されているか否かを判定し、暗号化されている場合には、所在情報暗号化鍵共有部1103において著作権保護システム1300との間で共有さ



れている鍵 1 1 0 7 を用いて、その暗号化されたコンテンツ所在情報及び所在認証情報を復号する。

【 0 0 4 8 】

コンテンツ配信サーバ検証部 1 1 1 3 は、受信したコンテンツ選択文書 1 4 0 0 から、所在認証情報タグに基づいて、所在認証情報を抽出する。次に、コンテンツ配信サーバ検証部 1 1 1 3 は、この所在認証情報に基づいてコンテンツの所在の正当性、換言すればコンテンツ配信サーバの正当性を判定する。コンテンツ配信サーバ検証部 1 1 1 3 は、コンテンツ配信サーバが正当であると判定した場合にのみ、コンテンツ配信要求部 1 1 0 4 へコンテンツ所在情報を出力する。コンテンツ配信要求部 1 1 0 4 は、このコンテンツ所在情報で指定されるコンテンツを保有するコンテンツ配信サーバに対し、コンテンツの配信要求を送信する。

【 0 0 4 9 】

この配信要求に応じてコンテンツ配信サーバからコンテンツが配信されると、コンテンツ受信部 1 1 0 5 は、このコンテンツを受信する。コンテンツ復号部 1 1 1 4 は、コンテンツを構成する符号化された音楽データや映像データを復号し、それぞれの出力デバイス（図示せず）へ音声信号や映像信号を出力する。なお、受信したコンテンツが暗号化されている場合には、コンテンツ暗号化復号部 1 1 0 9 は、その暗号化されたコンテンツを、コンテンツ暗号化鍵共有部 1 1 0 6 によってコンテンツ配信サーバとの間で共有されている鍵を用いて復号し、コンテンツ復号部 1 1 1 4 へ出力する。

【 0 0 5 0 】

上述した端末認証部 1 1 0 1、所在情報暗号化鍵共有部 1 1 0 3、コンテンツ配信要求部 1 1 0 4、コンテンツ暗号化鍵共有部 1 1 0 6、コンテンツ暗号化復号部 1 1 0 9、所在情報暗号化復号部 1 1 1 2、コンテンツ配信サーバ検証部 1 1 1 3 及びコンテンツ復号部 1 1 1 4 は、耐タンパー性を有するソフトウェア又はハードウェアで実装することにより、ユーザの不正操作を防止することができる。また、コンテンツ所在情報は、この耐タンパー性により、コンテンツ受信端末 1 1 0 0 のユーザを含め、外部への漏洩が防止される。

【 0 0 5 1 】

このように、本実施例のコンテンツ配信システム 1 0 0 0 では、著作権保護システム 1 3 0 0 は、暗号化部 1 3 0 9 がコンテンツ所在情報及び所在認証情報を暗号化し、コンテンツ文書生成部 1 3 1 0 が暗号化されたコンテンツ所在情報及び所在認証情報を複数組み合わせ合わせたコンテンツ選択文書を生成し、コンテンツ選択文書配信部 1 3 0 4 が生成されたコンテンツ選択文書をコンテンツ受信端末 1 1 0 0 へ送信する。一方、コンテンツ受信端末 1 1 0 0 は、コンテンツ選択文書受信部 1 1 0 2 が著作権保護システム 1 3 0 0 からのコンテンツ選択文書を受信し、所在情報暗号化復号部 1 1 1 2 が受信したコンテンツ選択文書から暗号化されたコンテンツ所在情報を抽出して復号し、コンテンツ配信サーバ検証部 1 1 1 3 が受信したコンテンツ選択文書から所在認証情報を抽出してコンテンツの所在の正当性を検証し、コンテンツ配信要求部 1 1 0 4 が検証によりコンテンツの所在の正当性が確認された場合にコンテンツの配信要求を送出し、コンテンツ受信部 1 1 0 6 がこの配信要求に応じてコンテンツサーバから配信されるコンテンツを受信する。

#### 【 0 0 5 2 】

従って、コンテンツ配信サーバと著作権保護システム 1 3 0 0 が分離され、且つ、コンテンツの配信に際してコンテンツ配信サーバと著作権保護システム 1 3 0 0 との間で情報のやり取りが行われることがないため、コンテンツ配信サーバの負荷を軽減させて、大規模なコンテンツ配信システムを構築することができる。

#### 【 0 0 5 3 】

また、従来のようにコンテンツ選択文書全体が暗号化されるのではなく、コンテンツ所在情報だけを選択的に暗号化されるため、課金種別に応じて暗号化された複数のコンテンツ所在情報をコンテンツ選択文書に含ませることで、効率的なコンテンツ課金を行うことができる。

#### 【 0 0 5 4 】

更に、コンテンツ所在情報を暗号化することにより、第三者がコンテンツを利用することを防止することができるため、従来のように、コンテンツ配信サーバにおいて必ずしもコンテンツを暗号化する必要はない。このため、コンテンツ受

信端末 1 1 0 0 は、暗号化されたコンテンツの復号処理を省略することができ、演算量の軽減を図ることが可能となる。

【 0 0 5 5 】

また、著作権保護システム 1 3 0 0 からコンテンツ受信端末 1 1 0 0 へコンテンツの所在の正当性を証明する所在認証情報とが送信されるため、コンテンツ受信端末 1 1 0 0 は、コンテンツ所在情報で示されるコンテンツの所在の正当性を検証することができ、不正なサーバへアクセスして配信を受けることが防止され適切な課金処理を行うことができる。

【 0 0 5 6 】

図 4 は、本発明の第 2 実施例に係るコンテンツ配信システムの構成例を示す図である。同図に示す同図に示すコンテンツ配信システム 2 0 0 0 は、コンテンツ受信端末 2 1 0 0 と、著作権保護システムとコンテンツ配信サーバとが同一のサーバに実装された著作権保護システム兼コンテンツ配信サーバ 2 2 0 0 とを備えて構成される。コンテンツ受信端末 2 1 0 0 と、著作権保護システム兼コンテンツ配信サーバ 2 2 0 0 とは、ネットワーク 2 4 0 0 を介して接続される。

【 0 0 5 7 】

著作権保護システム兼コンテンツ配信サーバ 2 2 0 0 は、図 1 に示した第 1 実施例における著作権保護システム 1 3 0 0 と同様、オーディオビジュアルデータであるコンテンツの所在を示すコンテンツ所在情報を暗号化し、この暗号化されたコンテンツ所在情報、コンテンツの所在の正当性を証明する所在認証情報、及び送信元である著作権保護システム兼コンテンツ配信サーバ 2 2 0 0 の正当性を証明する署名を含んだコンテンツ選択文書 2 3 0 0 を生成し、コンテンツ受信端末 2 1 0 0 へ配信する。

【 0 0 5 8 】

コンテンツ受信端末 2 1 0 0 は、図 1 に示した第 1 実施例におけるコンテンツ受信端末 1 1 0 0 と同様、受信したコンテンツ選択文書 2 3 0 0 に含まれている署名の検証、ユーザが選択したコンテンツに対応するコンテンツ所在情報の復号、コンテンツの所在の正当性の判定を行った上で、コンテンツ所在情報で指定されるコンテンツの配信要求を著作権保護システム兼コンテンツ配信サーバ 2 2 0

0へ送信し、この配信要求に応じて配信されるコンテンツを受信する。

【0059】

このように、著作権保護システムとコンテンツ配信サーバとが同一のサーバに実装されるようにしても良い。この場合、コンテンツ所在情報は、サーバ内のアドレス情報又はディレクトリ情報となる。

【0060】

図5は、本発明の第3実施例に係るコンテンツ配信システムの構成例を示す図である。同図に示す同図に示すコンテンツ配信システム3000は、コンテンツ受信端末3100、著作権保護システム3200、コンテンツサーバ群3400、コンテンツホルダ3600を備えて構成される。コンテンツ受信端末2100と、著作権保護システム3200及びコンテンツ配信サーバ3400とは、ネットワーク3500を介して接続される。

【0061】

コンテンツホルダ3600は、オーディオビジュアルデータであるコンテンツの所在を示すコンテンツ所在情報や該コンテンツに関連するアクセス制御情報（課金情報等）を含んだコンテンツ選択文書3700を生成し、著作権保護システム3200へ送信する。

【0062】

著作権保護システム3200は、受信したコンテンツ選択文書3700をコンテンツ受信端末3100へ送信するためのコンテンツ選択文書3300に変換する。この際、著作権保護システム3200は、コンテンツの所在の正当性を証明する所在認証情報の付与、アクセス情報に基づくコンテンツ所在情報の暗号化、コンテンツ選択文書の送信元となる著作権保護システム3200の正当性を証明する署名を付与する。なお、コンテンツホルダ、コンテンツサーバ運営者が所在認証情報を発行するようにしても良い。

【0063】

コンテンツ受信端末3100は、図1に示した第1実施例におけるコンテンツ受信端末3100と同様、受信したコンテンツ選択文書3300に含まれている署名の検証、ユーザが選択したコンテンツに対応するコンテンツ所在情報の復号

、コンテンツの所在の正当性の判定を行った上で、コンテンツ所在情報で指定されるコンテンツの配信要求をコンテンツ配信サーバへ送信し、この配信要求に応じて配信されるコンテンツを受信する。

#### 【 0 0 6 4 】

なお、上述した第1乃至第3の実施例では、著作権保護システムはコンテンツ所在情報及び所在認証情報の双方を暗号化したが、コンテンツ所在情報のみを暗号化しても良い。

#### 【 0 0 6 5 】

ところで、上述したように、コンテンツ選択文書にはコンテンツの所在の正当性を証明する所在認証情報や暗号化されたコンテンツ所在情報を埋め込む必要がある。これら所在認証情報や暗号化されたコンテンツ所在情報の埋め込みには、インターネット上で交換されるデータの記述言語として一般的になりつつあるXML (eXtensible Markup Language) を利用することができる。

#### 【 0 0 6 6 】

XMLは、ユーザがタグを自由に定義することができる汎用的なデータ記述言語であり、所在認証情報であることを示すタグ(所在認証情報タグ)やコンテンツ所在情報が暗号化されていることを示すタグ(暗号化情報タグ)をも定義することができる。また、W3Cでは、文書の一部に対する署名を実現することができるXML-signatureの標準化が進められている。このXML-signatureは、署名に関する情報をタグ付けし、XML文書で表すための規格であり、htmlやXMLの文書の中にテキスト形式で署名情報を埋め込むことを可能にしている。このため、所在認証情報や暗号化されたコンテンツ所在情報の埋め込みにXMLを利用することが可能となる。

#### 【 0 0 6 7 】

図6は、XML-signatureの構造を示す図である。同図に示すようにXML-signatureはSignatureエレメント4000で始まる。このSignatureエレメント4000は、SignedInfoエレメント4100、Signature Valueエレメント4200、Key Infoエレメント4300からなる。ここで、SignedInfoエレメン

ト 4 1 0 0 には、署名に用いられるアルゴリズム、個々の署名対象の U R I、署名対象のハッシュ値が含まれる。S i g n a t u r e V a l u e エレメント 4 2 0 0 は、S i g n e d I n f o エレメント 4 1 0 0 についての署名値であり、S i g n e d I n f o エレメント 4 1 0 0 が改竄されていないことを証明する。K e y I n f o エレメント 4 3 0 0 は、署名値を検証するための鍵データである。

#### 【 0 0 6 8 】

コンテンツの所在の正当性を証明する所在認証情報の埋め込みに X M L - s i g n a t u r e を利用する場合、認証局又は著作権保護システムで生成されたコンテンツ配信サーバに対する証明情報の U R I を R e f e r e n c e エレメント 4 1 3 0 に、この証明情報から生成される認証情報を S i g n a t u r e V a l u e エレメント 4 2 0 0 にそれぞれ埋め込む。また、認証情報を生成するために使用したアルゴリズムを S i g n e d I n f o エレメント 4 1 0 0 に、認証情報を検証するための鍵とその鍵の共有方法とを K e y I n f o エレメント 4 3 0 0 にそれぞれ埋め込む。

#### 【 0 0 6 9 】

また、暗号化されたコンテンツ所在情報をコンテンツ選択文書に埋め込む場合には、I B M 東京基礎研究所の村山氏らが提案する E l e m e n t - W i s e X M L E n c r y p t i o n (<http://lists.w3.org/Archives/Public/xml-encryption/2000Apr/att-0005/01-xmlenc> 参照) 等を利用することができる。本提案は、XML 文書のエレメント単位で暗号化を施すことを可能にするものであり、図 7 に示すように、暗号化エレメント内に暗号文と暗号化に用いたアルゴリズムとを埋め込むことができる。

#### 【 0 0 7 0 】

上記各例において、著作権保護システム 1 3 0 0 内の暗号化部 1 3 0 9 が暗号化手段に、コンテンツ文書生成部 1 3 1 0 がコンテンツ選択文書生成手段に、コンテンツ選択文書配信部 1 3 0 4 がコンテンツ選択文書送信手段に対応する。また、コンテンツ受信端末 1 1 0 0 内のコンテンツ選択文書受信部 1 1 0 2 がコンテンツ選択文書受信手段に、所在情報暗号化復号部 1 1 1 2 がコンテンツ所在情

報を抽出手段及び復号手段に、コンテンツ配信サーバ検証部 1 1 1 3 が所在認証情報抽出手段及び正当性検証手段に、コンテンツ配信要求部 1 1 0 4 が配信要求送出手段に、コンテンツ受信部 1 1 0 6 がコンテンツ受信手段に対応する。

#### 【0071】

##### 【発明の効果】

上述の如く、本願発明によれば、コンテンツ配信サーバと著作権保護システムが分離され、且つ、コンテンツの配信に際してコンテンツ配信サーバと著作権保護システムとの間で情報のやり取りが行われることがないため、コンテンツ配信サーバの負荷を軽減させて、大規模なコンテンツ配信システムを構築することができる。

#### 【0072】

また、従来のようにコンテンツ選択文書全体が暗号化されるのではなく、コンテンツ所在情報だけを選択的に暗号化することが可能であるため、例えば課金種別に応じて暗号化された複数のコンテンツ所在情報をコンテンツ選択文書に含ませることで、効率的なコンテンツ課金を行うことができる。

#### 【0073】

また、著作権保護システムからコンテンツ受信端末へコンテンツの所在の正当性を証明する所在認証情報が送信されるため、コンテンツ受信端末は、コンテンツ所在情報で示されるコンテンツの所在の正当性を検証することができ、不正なサーバへアクセスして配信を受けることが防止され適切な課金処理を行うことができる。

#### 【0074】

特に、コンテンツ選択文書に課金種別等のコンテンツへのアクセス制御情報を付与することで、著作権保護システムがコンテンツ所在情報に対する暗号化を適切に行うことが可能になる。

##### 【図面の簡単な説明】

#### 【図1】

第1実施例に係るコンテンツ配信システムの構成例を示す図である。

#### 【図2】

第 1 実施例に係る著作権保護システムの構成例を示す図である。

【図 3】

第 1 実施例に係るコンテンツ受信端末の構成例を示す図である。

【図 4】

第 2 実施例に係るコンテンツ配信システムの構成例を示す図である。

【図 5】

第 3 実施例に係るコンテンツ配信システムの構成例を示す図である。

【図 6】

XML - S i g n a t u r e の構造を示す図である。

【図 7】

E l e m e n t - W i s e X M L E n c r y p t i o n の手順を示す図である。

【図 8】

コンテンツ配信サーバが認証、課金を行わない場合の従来のコンテンツ配信システムの構成例を示す図である。

【符号の説明】

- 1 0 0 0 コンテンツ配信システム
- 1 1 0 0 コンテンツ受信端末
  - 1 1 0 1 端末認証部
  - 1 1 0 2 コンテンツ選択文書受信部
  - 1 1 0 3 所在情報暗号化鍵共有部
  - 1 1 0 4 コンテンツ配信要求部
  - 1 1 0 5 コンテンツ受信部
  - 1 1 0 6 コンテンツ暗号化鍵共有部
  - 1 1 0 7 鍵
  - 1 1 0 8 コンテンツ選択文書検証部
  - 1 1 0 9 コンテンツ暗号化復号部
  - 1 1 1 0 コンテンツ選択メニュー表示部
  - 1 1 1 1 ユーザ選択受信部



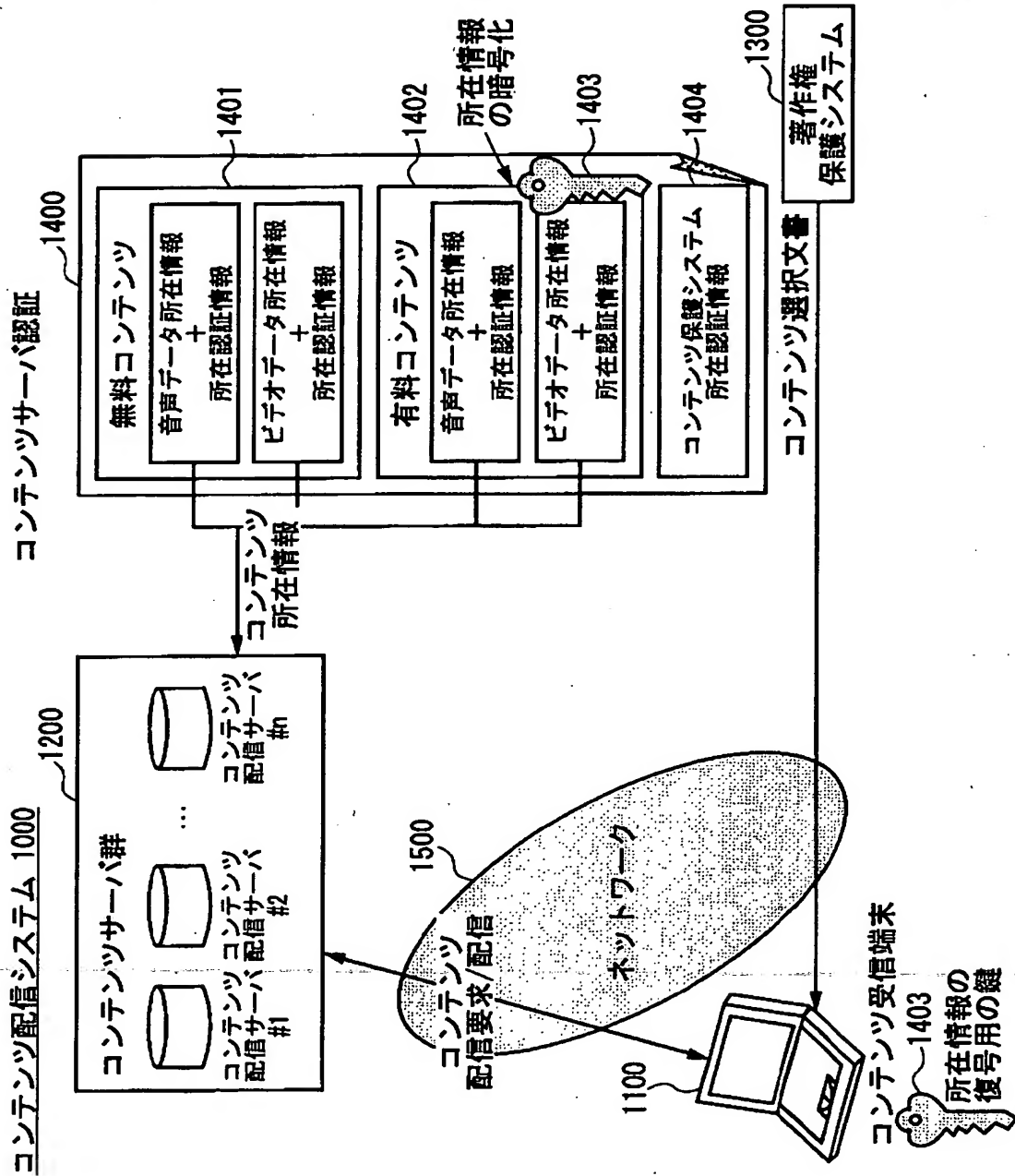
- 1 1 1 2 所在情報暗号化復号部
- 1 1 1 3 コンテンツ配信サーバ検証部
- 1 1 1 4 コンテンツ復号部
- 1 2 0 0 コンテンツサーバ群
- 1 3 0 0 著作権保護システム
- 1 3 0 1 アクセス情報受信部
- 1 3 0 2 端末認証部
- 1 3 0 3 所在情報暗号化鍵共有部
- 1 3 0 4 コンテンツ選択文書受信部
- 1 3 0 5 課金情報蓄積サーバ
- 1 3 0 6 課金部
- 1 3 0 7 鍵
- 1 3 0 8 コンテンツ所在情報
- 1 3 0 9 暗号化部
- 1 3 1 0 コンテンツ選択文書生成部
- 1 3 1 1 所在認証情報
- 1 3 1 2 所在認証情報タグ付加部
- 1 3 1 3 署名部
- 1 3 1 4 情報付加部
- 1 4 0 0 コンテンツ選択文書
- 1 5 0 0 ネットワーク

【書類名】

図面

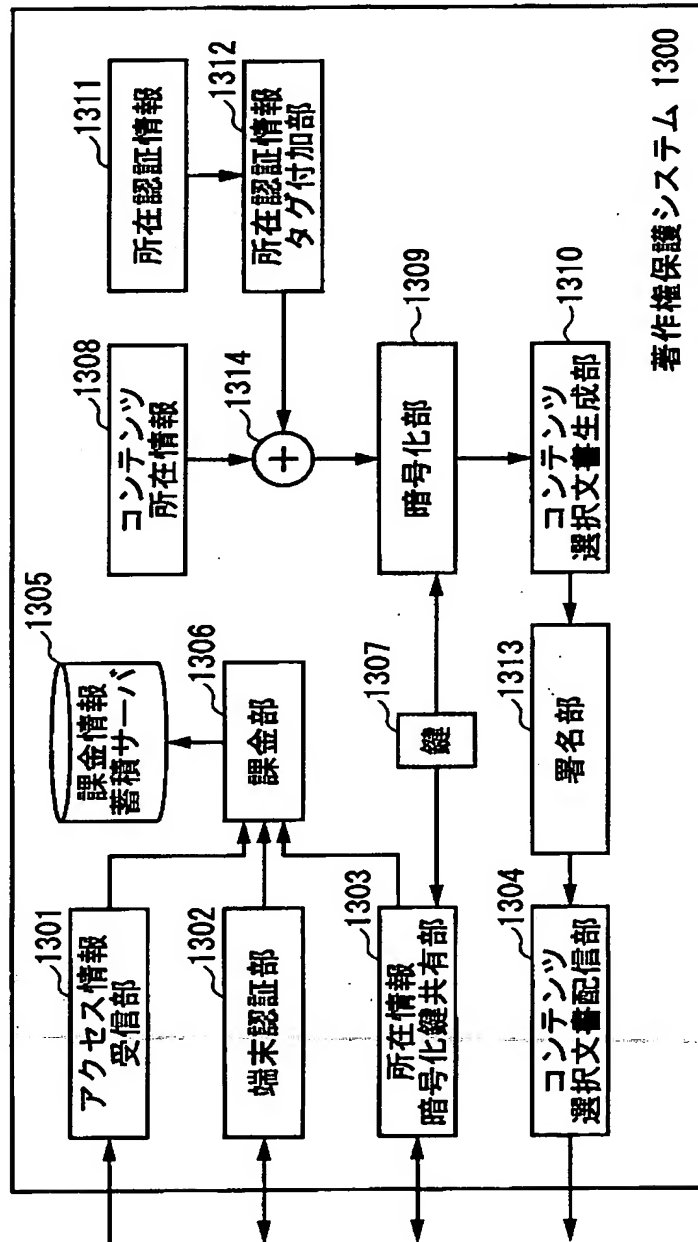
【図 1】

第 1 実施例に係るコンテンツ配信システムの構成例を示す図



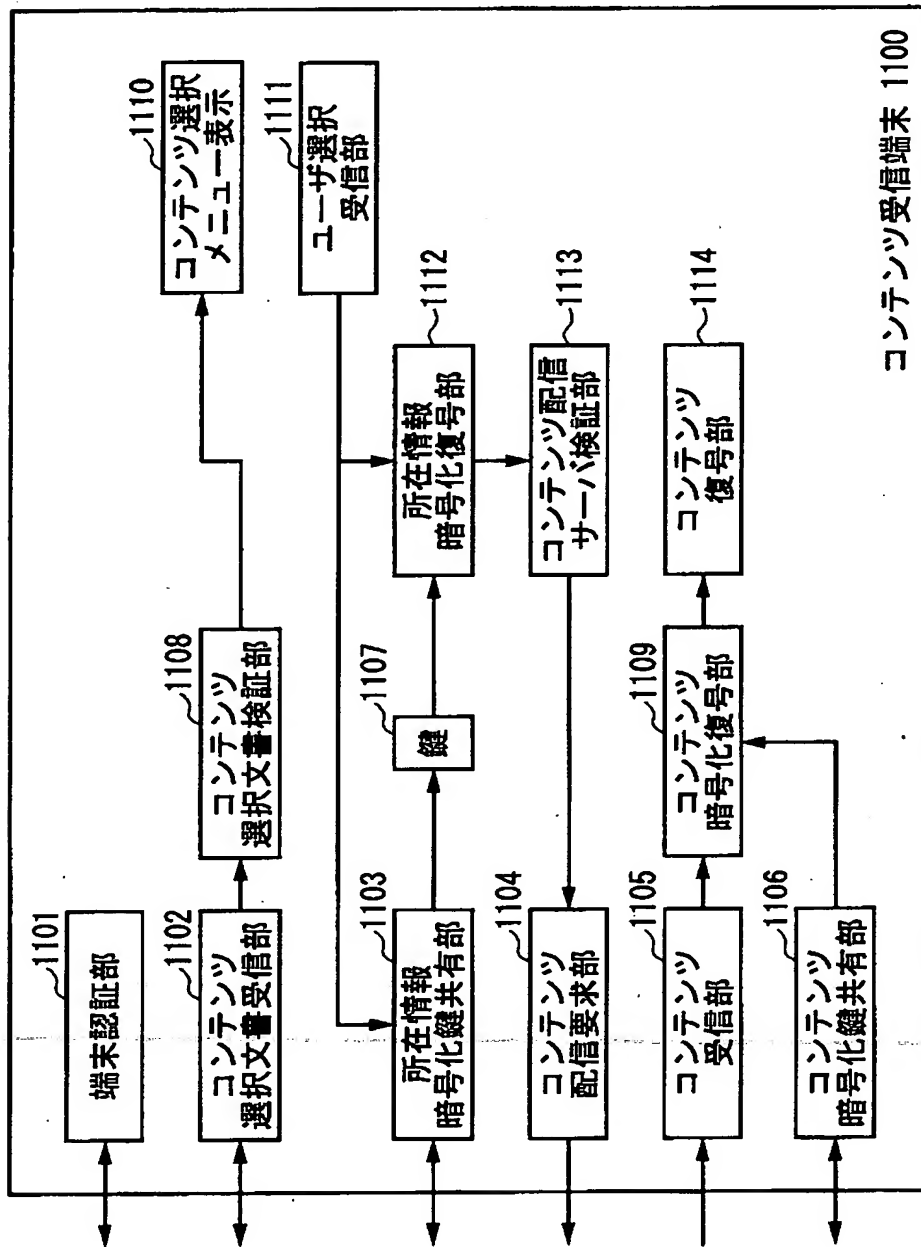
【図2】

第1実施例に係る著作権保護システムの構成例を示す図



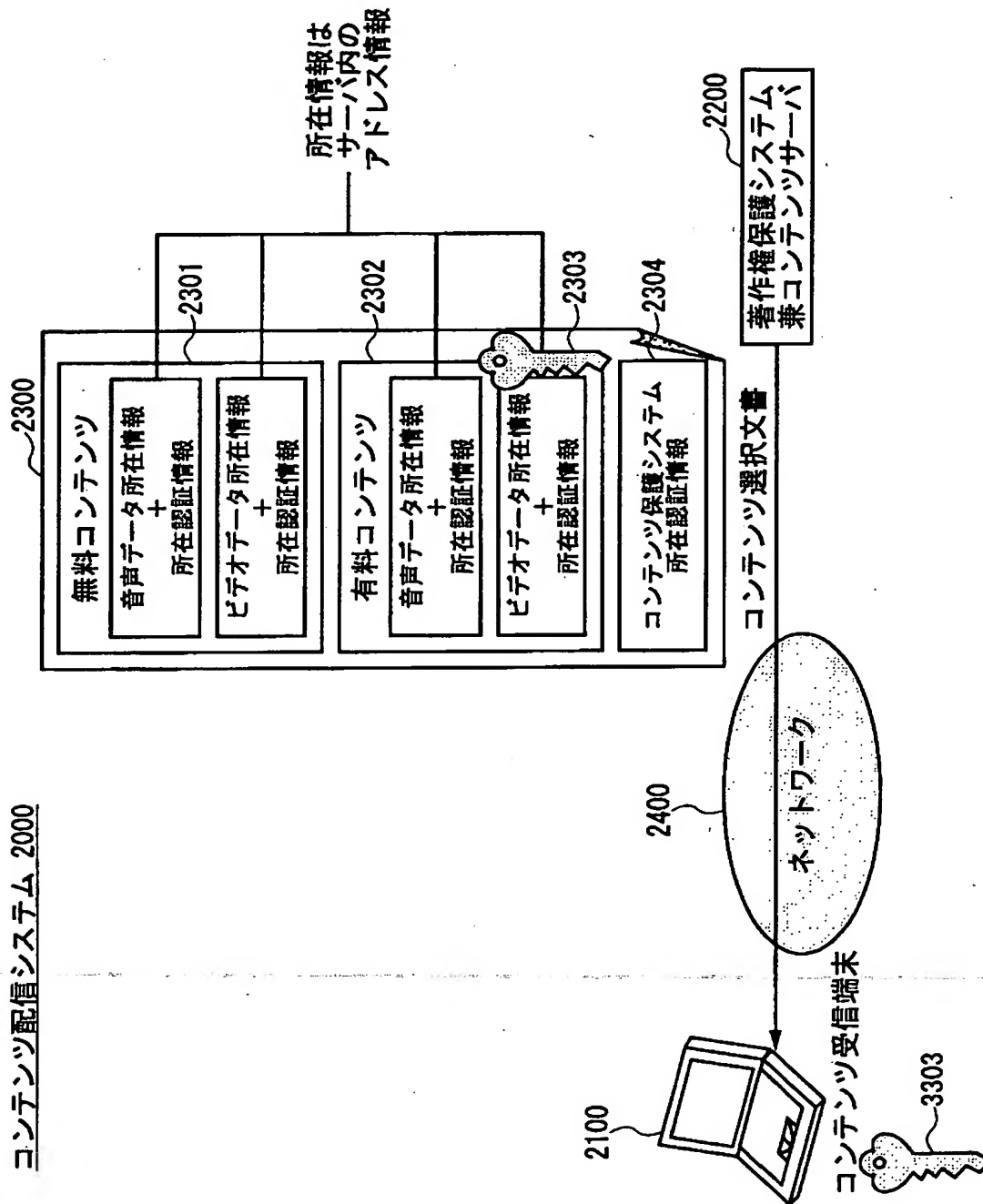
【図3】

第1実施例に係るコンテンツ受信端末の構成例を示す図



【図 4】

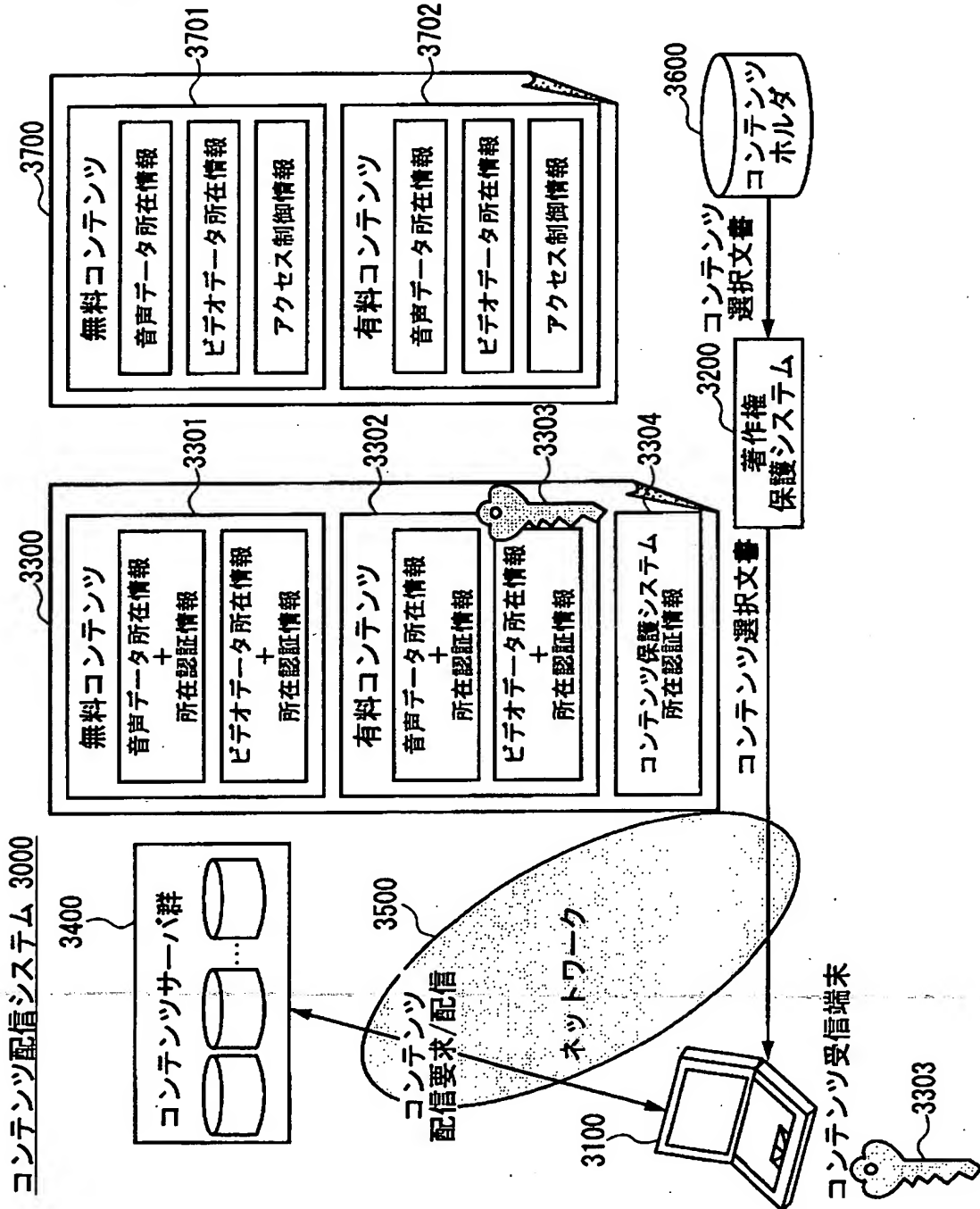
第 2 実施例に係るコンテンツ配信システムの構成例を示す図



コンテンツ配信システム 2000

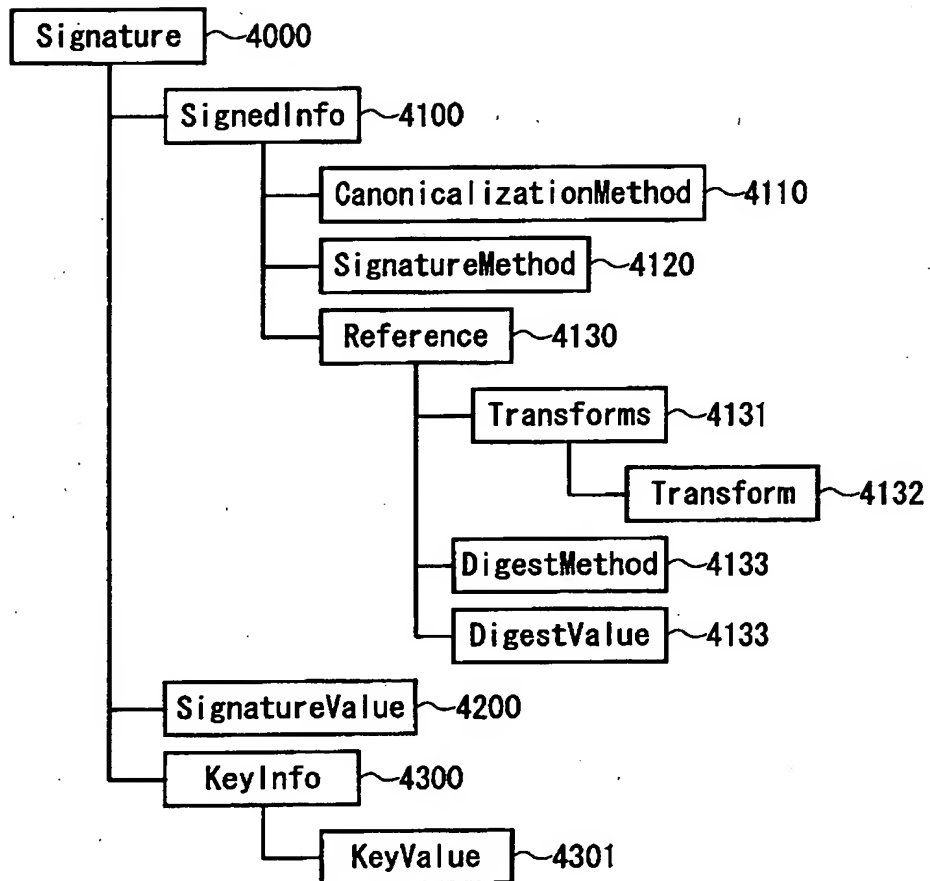
【図 5】

第3実施例に係るコンテンツ配信システムの構成例を示す図



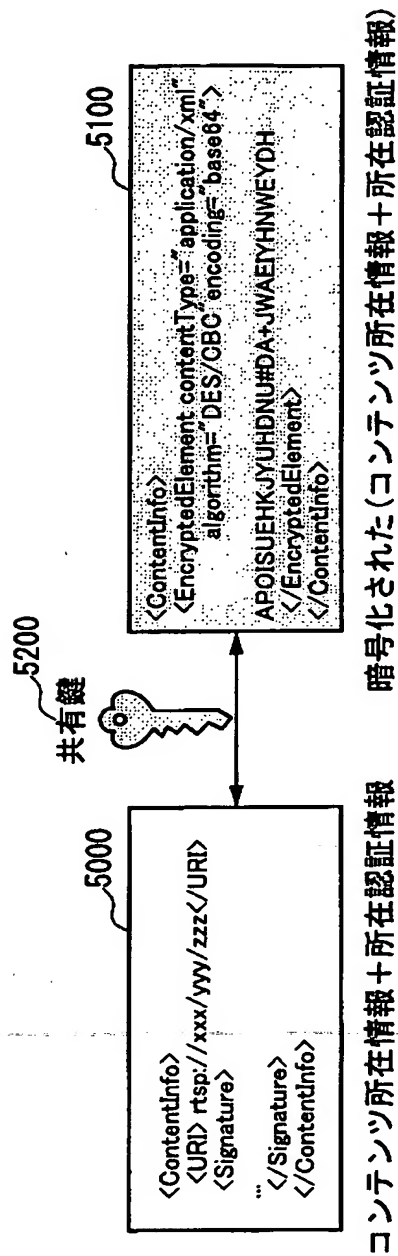
【図 6】

XML-Signature の構造を示す図



【図 7】

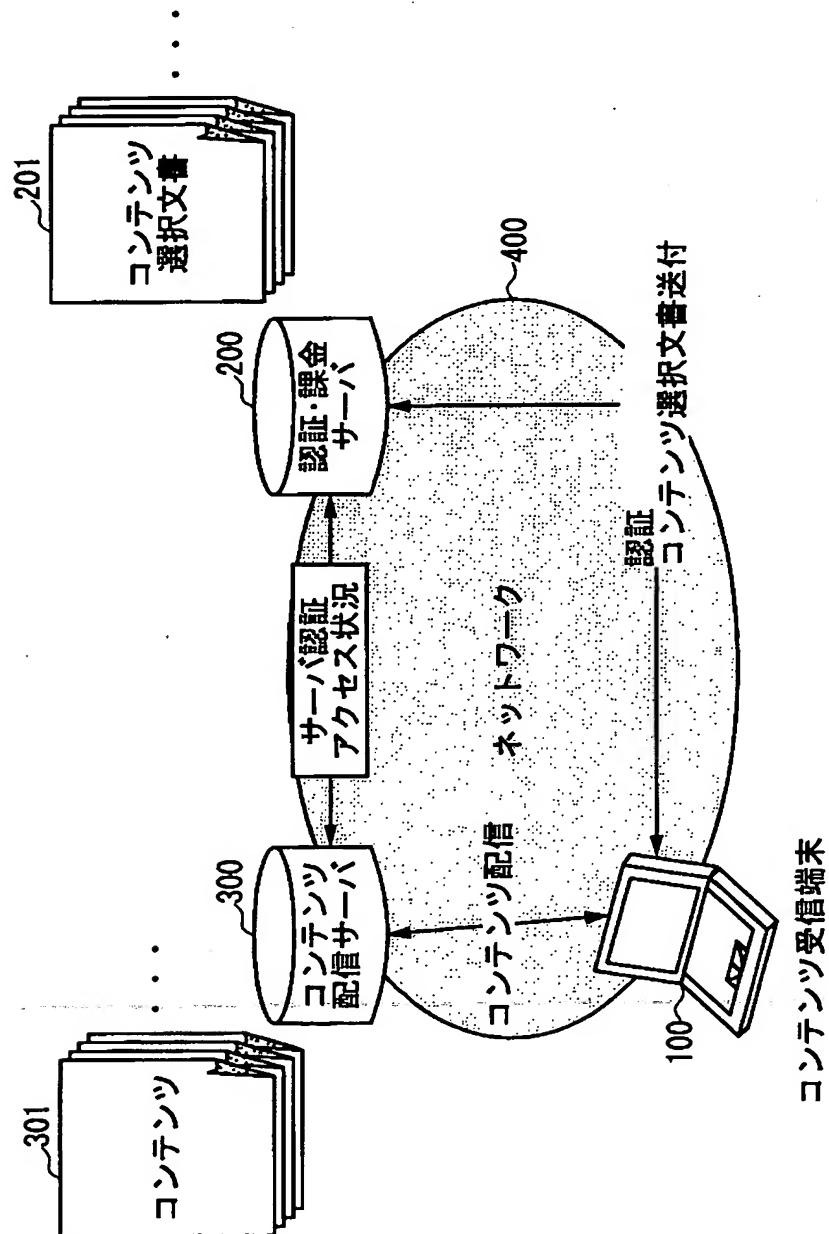
Element-Wise XML Encryptionの手順を示す図





【図 8】

コンテンツ配信サーバが認証、課金を行わない場合の  
従来のコンテンツ配信システムの構成例を示す図



【書類名】 要約書

【要約】

【課題】 大規模なシステムを構築可能であるとともに、コンテンツ課金を適正に行うことができるコンテンツ配信システム、著作権保護システム及びコンテンツ受信端末を提供する。

【解決手段】 著作権保護システム 1 3 0 0 は、所在認証情報が付加されたコンテンツ所在情報を暗号化し、この暗号化したコンテンツ所在情報と所在認証情報とを含んだコンテンツ選択文書を生成してコンテンツ受信端末 1 1 0 0 へ送信する。コンテンツ受信端末 1 1 0 0 は、このコンテンツ選択文書を受信し、暗号化されたコンテンツ所在情報及び所在認証情報を抽出して復号し、所在認証情報によりコンテンツの所在の正当性を検証し、コンテンツの所在の正当性が確認された場合にコンテンツ所在情報で指定されるコンテンツ配信サーバに対し配信要求を送出し、この配信要求に応じて配信されるコンテンツを受信する。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [392026693]

1. 変更年月日 2000年 5月19日  
[変更理由] 名称変更  
住 所 東京都千代田区永田町二丁目11番1号  
氏 名 株式会社エヌ・ティ・ティ・ドコモ